3GPP TSG-RAN WG2 #109bis-e R2-20xxxxx

Electronic Meeting, April 20th – 30th 2020

Agenda Item: 5.4.1.1

Source: Ericsson

Title: [AT109bis-e][008][NR15] Conn Control Miscellaneous I

Document for: Discussion, Decision

# 1 Introduction

This document is to kick off the following email discussion:

* [AT109bis-e][008][NR15] Conn Control Miscellaneous I (Nokia, Ericsson, CATT, Huawei)

Scope: Treat R2-2002681, R2-2002682, R2-2002683, R2-2003071, R2-2003386, R2-2003196, R2-2003197, R2-2002787, R2-2003480, R2-2003483,

Part 1: Determine which issues that need resolution, find agreeable proposals. Deadline: April 23 0700 UTC

Part 2: For the parts that are agreeable, discussion will continue to agree on CRs.

# 2 Discussion

Companies are requested to add their comments for each of the treated CRs of this email discussion in the boxes below (one for each CR to be treated).

### 2.1 Discussion on recursion in RRC ([R2-2002681](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002681))

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Ericsson | Disagree | Our understanding is that there is no such a issue for Rel-15. Even if in Rel-16 we assume that a possible network implementation will implement the scenario described by Nokia, such scenario has never been described in any stage 2 and stage 3 spec. Therefore, we think that this should not be a problem. |
| Nokia, Nokia Shanghai Bell | Agree | Rel-15 already allows recursion as the document explains, and the recursion has already been discussed under CHO for Rel-16. This may create hard-to-track cases for UE behaviour and create potential difficulties in the field.  Hence, it would be better to clarify the topic now and we would at least like to understand if UEs support the recursion up to an arbitrary level?  Additionally, having the references inside OCTET STRINGs can cause issues with some ASN.1 tools in case they check the contents, as the recursion requires manual removal of the "CONTAINING XXX" to work. Having the note in the field description allows finding those cases more easily. |
| ZTE | Need time to check | We haven’t seen any problem so far, in our understanding, at least the problematic scenarios mentioned by Nokia is not supported in Rel-15 (e.g. the RRCReconfiguration in mrdc-SecondaryCellGroup will not contain another contained message).  For Rel-16, if such recursion is required (e.g. CHO), we are not sure whether there is issue with ASN.1 tools, it is better to allow more time to check. But even if the problem exists, we are wondering whether adding restriction to spec is the only way to solve it? |
| Apple | Agree | We share the same view of Nokia. The recursive RRC messages with the same name create problems in ASN.1 decoder and may lead to a looping attack. It is necessary to clarify the usage constraints of this recursive syntax. |
| CATT | Disagree | There is no such issue, it specifies that for the RRCReconfiguration in the mrdc-SecondaryCellGroup can only include the secondaryCellGroupConfig and measConfig, so there is no recursion. |
| Samsung | Disagree | We think there seems no real problem with the current text. |
| MediaTek | See comment | We agree that UE or NW does not includes the recursion of RRC message in arbitrary level. Thus, we are fine with the intention. However, we also think that with or without any SPEC change, it is almost impossible that implementation will consider the current SPEC as multiple level of recursion. |
| Intel | May be | We don’t see it as essential as we dont see a risk with Rel-15 spec. Although the ASN.1 itself may not prevent it, the rest of the specification should be clear. |
| NTT DOCOMO | Agree but | Such a risk of infinite loop may not be a real problem, although it may happen from ASN.1 coding viewpoint. We’re fine with give a clarification in the spec. |

### 2.1.1 Clarification on recursion in RRC messages ([R2-2002682](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002682), [R2-2002683](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002683), [R2-2003071](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003071))

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Ericsson | Disagree | Our understanding is that there is no such a issue for Rel-15. Even if in Rel-16 we assume that a possible network implementation will implement the scenario described by Nokia, such scenario has never been described in any stage 2 and stage 3 spec. Therefore, we think that this should not be a problem. |
| Nokia, Nokia Shanghai Bell | Agree | Rel-15 already allows recursion as the document explains, and the recursion has already been discussed under CHO for Rel-16. This may create hard-to-track cases for UE behaviour and create potential difficulties in the field.  Hence, it would be better to clarify the topic now and we would at least like to understand if UEs support the recursion up to an arbitrary level?  Additionally, having the references inside OCTET STRINGs can cause issues with some ASN.1 tools in case they check the contents, as the recursion requires manual removal of the "CONTAINING XXX" to work. Having the note in the field description allows finding those cases more easily. |
| ZTE | Need time to check | We haven’t seen any problem so far, in our understanding, at least the problematic scenarios mentioned by Nokia is not supported in Rel-15 (e.g. the RRCReconfiguration in mrdc-SecondaryCellGroup will not contain another contained message).  For Rel-16, if such recursion is required (e.g. CHO), we are not sure whether there is issue with ASN.1 tools, it is better to allow more time to check. But even if the problem exists, we are wondering whether adding restriction to spec is the only way to solve it? |
| Apple | Agree | Share the same view with Nokia |
| CATT | Disagree | There is no such issue, it specifies that for the RRCReconfiguration in the mrdc-SecondaryCellGroup can only include the secondaryCellGroupConfig and measConfig, so there is no recursion. |
| Samsung | Disagree | We think there seems no real problem with the current text. |
| MediaTek | Maybe | We think current text is fine. The proposed change is also OK but I will assume that implementer already take this kind of assumption. So, not critical to have this. |
| Intel | May be | Please see comment above. |
| NTT DOCOMO | Agree but | Please see comment above |

## 2.2 Piggybacking of NAS PDUs including Service Accept ([R2-2003386](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003386))

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Nokia | Disagree | This seems potentially related to the earlier discussion with CT1/RAN3. We do not see a concrete proposal so difficult to say what is broken and what is the intended fix for that. Indeed, the list size may in very theoretical cases be limiting but the real issue just seems to stem from a matter of implementation choice? We do not support this as there is no real show-stopper. It would be better to discuss this at CT1 first and get their consensus. |
| Ericsson | Agree | Nothing is broken and we (Ericsson) do not propose to change the specification in any way.  The intention of the paper is for RAN2 to confirm that it is possible to piggyback the NAS PDU containing Service Accept. It is our understanding that this is allowed, and we want to hear other companies views on whether they think it is allowed or not.  As said, we dont propose to change the specification in any way, so we think it is sufficient to capture in MoM that piggybacking of Service Accept is allowed. |
| ZTE | Agree | We agree with the two proposals. |
| Apple | Not sure | The text in RRC is ok, it does not prevent the NW from piggybacking the service accept message in RRCReconfigure. So, not sure why RAN2 need explicitly single out this specific case for a discussion.  Regarding the size of piggyback list, if there is no CR needed, we do not see the need of a discussion, either. |
| CATT | Disagree, but | This should not be a problem. 256 is just RAN3’s fashion (RAN3 tends to avoid extending the max length of a list), it does not mean these is such case.  In addition, we share the same view that it is possible to piggyback the NAS PDU containing Service Accept. |
| Samsung | Disagree | If the intention is just to conform whether Proposal 1 is agreeable, our answer is yes. But other than that, we think no further discussion is needed as expressed by other companies. |
| MediaTek | See comment | We are OK with proposal 1 and we could capture something in Chairman’s Note based on this.  For proposal 2, we think nothing is needed. Don’t know why we have to confirm a “bottleneck”.  In any case, we prefer not to change the current specification. |
| Intel | See comment | Nothing is forbidden from RRC point of view. The way RRC is designed, it is up to the network to decide what can be piggybacked - that is, if it requires joint success failure. It is up to network to ensure that the DRBs and the appropriate NAS PDUs are put together.  Regarding the number of NAS PDUs, it is not unusual for there to be different limits over different interfaces. If at all it were to happen that more than 15 PDU sessions were to be established, then network can send two RRC reconfiguration messages. In summary, while the observations in the document are correct, there is no real issue here to solve. " |
| NTT DOCOMO | Agree on Prop.1 | Not sure about Proposal 2, although the scenario explained in the paper is a likely scenario. |

## 2.3 Correction related to RRC reconfiguration complete ([R2-2003196](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003196), [R2-2003197](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003197))

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Nokia | Disagree | Cannot see what is broken from the current specification as the packing of the reconfiguration complete is quite basic functionality and even for EN-DC this is quite clear. |
| Ericsson | Agree | We just want to clarify that the first change it concerns NR-DC and, in this case, there may be confusion as both the MCG RRCReconfiguration and the SCG RRCReconfiguration are both NR. For this reason, we would like to make clear which message is embedded in which one.  For the second change, the word ”submit” is wrong as the actual submission of the message is done in the LTE specification. Therefore, is order to not create any measleading behaviour would be good to align the terminology to that one that is used in 36.331. |
| ZTE | Disagree | We understand the intention, but seems the original wording hardly causes misunderstanding, because it is common understanding that MCG’s RRC Complete cannot be contained in SCG’s RRC Complete message.  If we really need to make this clear enough in spec, we are afraid the current CR does not cover all the cases yet. |
| Apple | Disagree | For NR-DC, It is very clear the encapsulated RRCReconfigurationComplete message is for SCG as the RRCReconfigure is embeded in an IE named “nr-scg”. For EN-DC, the only needed change is to replace “submit” with “include”. |
| CATT | Disagree | Agree with Nokia, the current spec is clear. And the change 1 is not correct, the text procedure is subject to the reconfiguration message which the UE is applied. If the following change is applied, the bullet 2> is subjected to the RRC reconfiguration message which is included in the mrdc-secondaryCellGroup,i.e. the RRC reconfigruatin message generated by SN, however the bullet 3> is subjected to the RRC reconfiguration message generated by MN.  *2> if the RRCReconfiguration message was included in the mrdc-SecondaryCellGroupConfig with mrdc-SecondaryCellGroup set to nr-SCG:*  *3> include the SCG RRCReconfigurationComplete message in the nr-SCG-Response within the MCG* |
| Samsung | Disagree | The CR is indeed correct but there seems no room for misunderstanding according to the current procedural text. If it is agreed, then it can be included in Rapporteur CR. |
| MediaTek | Disagree | We actually think current procedure is fine. The clarification is not really needed.  Also the first change is incorrect, it change the meaning of original text. |
| Intel | Disagree | The current text was discussed a few times already and updated and should be clear. |
| NTT DOCOMO | Disagree | We also agree on the intention of the proposal. On the other hand, it seems already clear and no room for misunderstanding at this stage? |

## 2.4 Correction on CSI-ResourceConfig ([R2-2002787](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2002787))

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Nokia | Disagree | Do not see a need to update the field description here. What is the exact problem and what is broken with the current text? |
| Ericsson | Disagree | We do not see any issue with the original text and thus we think the CR is not needed. |
| ZTE | Disagree | Agree with Nokia and Ericsson. |
| Apple | No strong view | It is sort of an editorial change. |
| CATT | Agree | csi-IM-ResourceSetlist are resources used for beam measurement and reporting in a CSI-RS resource set in current spec, but the resources are not used for beam management but for other CSI measurements, e.g. scheduling and MIMO operations. The description is not correct and should be changed to CSI measurement. Also, in the field description of nzp-CSI-RS-ResourceSetList, the purpose of the nzp-CSI-RS-ResourceSetList is not only for beam management but it is also for all types of CSI measurements, which is not accurate and requires correction |
| Samsung | Disagree | Same view with Nokia and Ericsson. |
| MediaTek | Disagree | Do not understand what is really changed. |
| Intel | Disagree | CR is not needed because there is no critical issue and in some cases, beam measurement is equivalent to CSI-RS measurement. |
| NTT DOCOMO | Disagree | Similar to the previous one, there is no room to incur any misinterpretation. |

## 2.5 Correction on PUSCH-less uplink carrier ([R2-2003480](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003480), [R2-2003483](https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_109bis-e/Docs/R2-2003483))

|  |  |  |
| --- | --- | --- |
| Company | Agree/Disagree | Comments |
| Nokia | Disagree | The definition was introduced based on the same company’s contribution we do not see any good reason to agree to this. The current specification text is fine, and we can live with the current definition and the "ambiguity" simply doesn't exist. |
| Ericsson | Disagree | This CR has been already treated in RAN2#108 and not pursued. Therefore, we should not discuss this again.  **From RAN2#108**  R2-1916081 Correction on PUSCH-less Scell Huawei, HiSilicon CR Rel-15 38.331 15.7.0 1417 - F NR\_newRAT-Core  - Nokia think we don’t need to clarify as this is not used anywhere else.  - Oppo agrees the change is not needed.  - Ericsson think we don’t use the word carrier in such contexts.  Comeback, check other related discussions  - Huawei indicate that for UP language was not changed  Not pursued |
| ZTE | Disagree | Agree with Ericsson. |
| Apple | Disagree | The change is not needed |
| Samsung | Disagree | Same view with Nokia and Ericsson. If anything needs to be fixed, we should at least keep the terminology itself but we can change the definition to include SUL i.e. PSUCH-less SCell: An SCell configured with UL without PUSCH. |
| MediaTek | Maybe | We think the change is fine but not essential. We also understand that this is already discussed in R2-1916081. It is decided as “Not pursued” at that time thus maybe we don’t need the CR. |
| Intel | Disagree | From RRC point of view, there is no motivation to change the definition. If it is really confusing for SUL, we could add additional description for SUL case. |
| NTT DOCOMO | Disagree | Same view as Nokia/Ericsson. |

# Conclusion

In the previous sections we made the following observations:

Based on the discussion in the previous sections we propose the following:

# References

[1]